SysAdmin's Notebook

Navigating the FortiGate BIOS

It doesn't happen often, though always more than we'd like, but sometimes we have to work in our FortiGate unit's BIOS. You should know in advance the capabilities of the BIOS. There is also the issue that there is more than one BIOS interface that you may be dealing with. This can be problematic if you are familiar with the features of one of them and expect to be able to do the same things in another BIOS. The purpose of this document is to point out what the differences in BIOS features and capabilities.

The Different BIOS versions

There are a number of BIOS version numbers but for the most part they don't change. Currently, a BIOS version can be placed in one of two categories:

- ### The Old BIOS

  This BIOS is currently on the bulk of the models. The TFTP setup is created from scratch each time it was used.

- ### The New BIOS

  The new BIOS started with a few models in 2013. The major change here is that the TFTP set up can be statically set to a default and the BIOS has the ability to connect to a TFTP server that is on a different subnet.

  There can be some confusion with some models, as depending on when the unit was built the same model could have either the older BIOS or the newer one. Currently, models that use the new BIOS include:

  - FortiGate / FortiWiFi 30D-PoE BIOS version greater than 04000002
  - FortiGate / FortiWiFi 60D BIOS version greater than 04000020
  - FortiGate / FortiWiFi 90D BIOS version greater than 04000016
  - FortiGate / FortiWiFi 90D-PoE BIOS version greater than 04000006

The BIOS Menus

The quickest way to tell whether or not you are dealing with an old or new BIOS is the initial menu display. You will notice that the new BIOS has a different list of options than the old BIOS.

The Initial Menu: Old BIOS

```
[G]: Get firmware image from TFTP server
[F]: Format boot device.
[I]: Configuration and information.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot.
[H]: Display this list of options.

Enter: G,F,I,B,Q,or H:
```

The Initial Menu: New BIOS

```
[C]: Configure TFTP parameters.
[R]: Review TFTP parameters.
[T]: Initiate TFTP firmware transfer.
[F]: Format boot device.
[I]: System information.
```

```
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot.
[H]: Display this list of options.

Enter C,R,T,F,I,B,Q,or H:
```

The Differences

Difference #1

```
[G]: Get firmware image from TFTP server
```

Has been replaced by the following 3 menu items:

```
[C]: Configure TFTP parameters.
[R]: Review TFTP parameters.
[T]: Initiate TFTP firmware transfer.
```

Difference #2

```
[I]: Configuration and information.
```

Has been replaced by

```
[I]: System information.
```

Tips for the Interface:

- When using the bracketed single letter options, the input is case insensitive.
- Be careful as to what you enter. There is no error checking for invalid input.
- [H] will redisplay the menu that you are in.
- [Q] will return you out of the existing menu to the previous one, but not back out of a setting configuration. The exception is [Q] in the main menu. There the command will exit from the BIOS menu and continue with the boot process.
- If a new value is given for most settings there is a short pause followed by the CLI displaying the message:

  ```
  ...done
  ```

- Pressing the Enter key without typing in a value will cause the system to use the default value in the square brackets.
- After the BIOS finishes an instruction the CLI will display the available options. For example:

  ```
  Enter P,D,I,S,G,V,T,F,R,N,Q,or H:
  ```

- Be careful about the selection entries. There are non-displayed options that are intended for Fortinet technicians. You don't want to get into a menu that could have unintended consequences if you enter the wrong input.

[G]: Get firmware image from TFTP server. **(Old version)**

```
Please connect TFTP server to Ethernet port 'WAN1'.

Enter TFTP server address [192.168.1.145]:
Enter local address [192.168.1.188]:
Enter firmware imagefile name [image.out]:
```

[C]: Configure TFTP parameters. **(New version)**

[P]: Set firmware download port.

The options listed will vary from model to model due to the different port variations but the objective is the same; you can control which of the ports to connect the Ethernet cable to. This eliminates the need for sophisticated routing tables so the TFTP client software in the BIOS only needs to monitor one interface. Also, you don't have to alter existing connections to perform the TFTP download.

```
[0]:  Any of port 1 - 7
[1]:  WAN1
[2]:  WAN2
Enter image download port number [WAN1]:
```

[D]: Set DHCP mode.

Enabling the DHCP client mode will all the FortiGate to acquire IP address information from a DHCP server running on the same subnet as the FortiGate unit.

```
Current Setting: <The Factory Default value will be Disabled>
Please select DHCP setting
[1]:  Enable DHCP
[2]:  Disable DHCP
```

After enabling the DHCP client a review of the TFTP settings will indicate:

```
Local IP address:       N/A
Local subnet mask:      N/A
Local gateway:          N/A
```

This is because the DHCP request has not been sent out at this point. The DHCP request goes out when the 'Initiate TFTP firmware transfer' command has been given.

[I]: Set local IP address.

Statically assigns the IP address on the download interface of the FortiGate. The IP address will be in the standard IPv4 format.

```
Enter local IP address [192.168.1.188]:
```

[S]: Set local subnet mask.

Statically assigns the subnet mask on the download interface of the FortiGate.

```
Enter local subnet mask [255.255.252.0]:
```

[G]: Set local gateway.

Statically assigns the IP address to be used as the default gateway on the download interface of the FortiGate. This allows the FortiGate to access a TFTP server on a different subnet than it is currently connected to.

[V]: Set local VLAN ID.

Statically assigns the VLAN ID to be used when in an environment that uses VLANs.

```
Enter local VLAN ID(-1 to set it none) [<NULL>]:
```

[T]: Set remote TFTP server IP address.

Statically assigns the IP address of the computer being used as a TFTP server. The IP address will be in the standard Ipv4 format. This allows the FortiGate to maintain an IP address for the server rather than entering it from scratch every time a firmware upgrade takes place.

```
Enter remote TFTP server IP address [192.168.1.145]:
```

[F]: Set firmware file name.

Statically assign the name of the image file to be downloaded from the TFTP server. There are two basic approaches to take with the image file:

1. Select a name for this option that is consistent and easy to remember, such as image.out, then change the name of the image file on the TFTP server to match. This requires a certain amount of administrative overhead on the TFTP server such as keeping a pool of firmware images in reserve and copying the one that is needed over to the TFTP server to rename and deleting it once it is downloaded as the next time a firmware image is needed it will be difficult to tell which firmware image to use based on the name of the file.
2. Change this entry every time a new image file has to be downloaded from the server.

```
Enter firmware file name [image.out]:
```

[E]: Reset TFTP parameters to factory defaults.

This will erase all the current TFTP parameters and replace them with the factory default values.

```
Perform the TFTP parameters factory reset? [Y/N]:
```

If [Y] is chosen there is a short pause followed by the CLI displaying the message:

```
...done
```

If [N] is chosen the option quits and returns to the previous menu.

[R]: Review TFTP parameters.

```
Image download port:    Any of port 1 - 7
DHCP status:            Disabled
Local VLAN ID:          <NULL>
Local IP address:       192.168.1.1
Local subnet mask:      255.255.255.0
Local gateway:          192.168.1.254
TFTP server IP address: 192.168.1.100
Firmware file name:     image.out
```

[N]: Diagnose networking(ping).

```
[1]: Ping remote TFTP server.
[2]: Ping gateway.
[3]: Ping specified IP address.
[Q]: Quit this menu.
[H]: Display this list of options.

Enter 1,2,3,Q,or H:
```

Example: Press [1] to ping TFTP server:

```
Ping#1: Host 192.168.1.100 is reachable.
Ping#2: Host 192.168.1.100 is reachable.
Ping#3: Host 192.168.1.100 is reachable.
Ping#4: Host 192.168.1.100 is reachable.
```

[R]: Review TFTP parameters. **(New version)**

See above

[T]: Initiate TFTP firmware transfer. **(New version)**

```
Please connect TFTP server to Ethernet port 'Any of port 1 - 7'.

MAC: 00:09:0f:b5:55:28

Connect to tftp server 192.168.1.145 ...

###########################################################
Image Received.
Checking image... OK
Save as Default firmware/Backup firmware/Run image without
saving:[D/B/R]?
```

Option [D]

```
Programming the boot device now.
.............................................................
.............................................................
.
Booting OS...
Reading boot image... 1239838 bytes
```

Depending on the status of the partition where the firmware will be stored, you may also get this message:

```
The system must reformat the boot device to install this
firmware.
The default and backup firmware will be lost.
Continue:[Y/N]?Y
```

Option [B]

```
Programming the boot device now.
.............................................................
.............................................................
.
Booting OS...
Reading boot image... 1239838 bytes
```

Option [R]

```
Booting OS...
Reading boot image... 1239838 bytes
```

Followed a few seconds later by the FortiGate unit coming up and being ready.

[F]: Format boot device. **(Both versions)**

```
It will erase data in boot device. Continue? [yes/no]:
```

The response must be in one of the two forms indicated. To format the device type ‘yes’ in full and in lower case, then press Enter. If everything worked correctly, the CLI displays the following message:

```
Formatting . . . . . Done.
```

[I]: Configuration and information. (Old version)

[S]: Set serial port baudrate(will take effect on next boot).

Statically assigns one of five standard speeds to the serial connection of the console port.

```
0:    9600
1:    19200
2:    38400
3:    57600
4:    115200
Enter baudrate option [9600]:
```

To set the value type the index value shown on the left rather than the actual baud rate shown on the right. If the wrong value is entered there is no error message. The value just fails to change. This setting will only set the data transmission speed of the serial connection.

[T]: Set image download port (will take effect now and on next boot).

This will temporarily assign an Ethernet port for the TFTP server to download the image file. After a second boot of the device the port will revert back to the default port.

The port options listed will vary from model to model due to the different port variations but the objective is the same; you can control which of the ports to connect the Ethernet cable to. This eliminates the need for sophisticated routing tables, so the TFTP client software in the BIOS only needs to monitor one interface. In addition it is not necessary to alter existing connections to perform the TFTP download.

```
[0]:  Any of port 1 - 7
[1]:  WAN1
[2]:  WAN2
Enter image download port number [WAN1]:
```

[C]: Set DHCP enable (will take effect now and on next boot).

```
[1]:  Enable DHCP
[2]:  Disable DHCP
Enter DHCP setting [Disabled]:
```

[I]: Display hardware information.

```
Vendor ID    : Fortinet
CPU family   : ARM9
CPU model    : arm926ejs
CPU MHz      : 800 MHz
Cache size   : 64 KB
Memory       : DDR SDRAM  2GB 1066MHz
Platform ID  : FGT60D
Serial number: FGT60D4613001043
BIOS Build   : FortiGate-60D (15:09-08.12.2013)
BIOS Ver:04000022
```

[I]: System information.

[S]: Set serial port baudrate(will take effect on next boot).

Same as old BIOS. See above.

[I]: Display hardware information.

Same as old BIOS. See above.

[B]: Boot with backup firmware and set as default. **(Both versions)**

If there is no firmware image set as the backup firmware the following message will be displayed:

```
Failed to mount filesystem. . .
Mount back up partition failed.
Back up image open failed.
Press 'Y' or 'y' to boot default image.
```

[Q]: Quit menu and continue to boot. **(Both versions)**

This option will exit the BIOS menu and continue with the boot process.

[H]: Display this list of options. **(Both versions)**

This option will redisplay the options of the current menu.

Upgrading BIOS

While upgrading the BIOS of a FortiGate device is possible, the risk commonly outweighs the potential gain. If anything goes wrong in the upgrade process there is a strong possibility of rendering your device unusable. This will likely require you to RMA your device, leaving your network with this important piece of hardware.

If, for some reason, there is a compelling reason to perform and upgrade it should not be done without the assistance of an experienced TAC technician, preferable L2 or above.